

Cato Surveillance Conference brings the Fourth Amendment into the information age

Defending Digital Privacy in a Pandemic

Americans are more dependent than ever on online services, as the COVID-19 pandemic has pushed grocery shopping, office work, and other daily activities into the digital realm. With that entanglement comes new concerns for privacy as large-scale data harvesting on an unprecedented level is being undertaken by both governments and private corporations. In December, experts came together to discuss these trends at the annual Cato Surveillance Conference, organized by senior fellow Julian Sanchez, whose work covers issues of technology, privacy, and civil liberties.

The daylong conference featured an opening keynote from Sen. Ron Wyden (D-OR), a longtime civil libertarian opponent of warrantless mass surveillance. He praised the role Cato has played in “continuing to prosecute the case in a bipartisan way” and spoke about his bill, cosponsored with Sen. Rand Paul (R-KY) and 18 other senators, to update the Electronic Communications Privacy Act of 1986. As Wyden explained, this law has left a massive loophole by allowing the government to evade court supervision and other legal limits by obtaining personal information from third-party vendors rather than directly from companies with a customer relationship. This practice of outsourcing mass surveillance that would be unlawful if done by the government itself would be ended by Wyden and Paul’s proposed the Fourth Amendment Is Not for Sale Act.

After the keynote, a panel moderated by Sanchez brought together two leading reporters to discuss their investigative work, Kashmir Hill of the *New York Times* and Dana Priest of the *Washington Post*. As part of her coverage of what has been dubbed the surveillance-industrial complex, Priest discussed how an Israeli company with government backing and approval



has been selling powerful spyware tools to authoritarian regimes. In the same vein, Hill’s reporting has revealed how the facial-recognition company Clearview AI has become a favorite of law enforcement, who use its supply of billions of photos that are harvested from the internet.

Other presentations included those of Julie Mao of Just Futures Law about government surveillance and retaliation against immigrant support groups and Elizabeth Laird of the Center for Democracy and Technology on the disturbing expansion of schools using spyware on students as part of the shift to virtual learning during the pandemic.

Jeff Kosseff, an associate professor of cybersecurity law at the U.S. Naval Academy, and Afsaneh Rigot, a fellow at Harvard University’s Technology and Public Purpose Project, explained how the demonization of anonymous speech online is misguided scapegoating at odds with the history and reality of how anonymity is a critical part of First Amendment freedoms.

In addition to the discussions, the conference also featured an unusual practical demonstration. Beau Woods of the Atlantic

Council first explained the security vulnerabilities of the so-called internet of things, the increasing usage of web access for common appliances and other things beyond traditional computers, including cars and medical devices. Deral Heiland, principal security researcher for cybersecurity firm Rapid7, then demonstrated these vulnerabilities in real time by hacking into a common consumer webcam such as the ones often used for home security.

Digital technology has opened up society in radical ways and enabled new kinds of human flourishing. But along with that promise comes the peril of new threats to freedom and privacy. Important decisions must be made about both public policy and private practices, with massive potential consequences for decades to come. With the annual Surveillance Conference, Cato continues to ensure that the timeless principles of limited government and individual liberty are applied faithfully to ever-evolving modern realities. ■

THE 2021 CATO SURVEILLANCE CONFERENCE CAN BE VIEWED AT CATO.ORG/EVENTS/CATO-SURVEILLANCE-CONFERENCE-2021.